Remarks and Arguments

Claims 1-11, 17-20 and 28-37 have been presented for examination. Claims 1-2, 4-6 and 8-11 have been amended.

Claims 1, 4-5, 7-9, 11, 17-18, 20, 34 and 36-37 have been rejected under 35 U.S.C. §103(a) over U.S. Patent No. 6,564,320 (de Silva, previously cited) in view of U.S. Patent No. 6,772,331 (Hind, previously cited.)

The point of the present invention is to tie certificates generated by a certificate authority to the registration authority that made the request for the certificate on behalf of a principal by including an identifier for the registration authority in the certificate. Since each certificate directly identifies the registration authority that requested that certificate, any certificate requested by that authority can be easily located and revoked. Thus, if a registration authority becomes untrustworthy and makes improper requests, any certificate requested by that authority can be efficiently revoked.

It is important to note that the registration authority sends both the request and its identifier to the certificate authority so that the identifier can be included in the certificate. For example, claim 1 has been amended to make it clear which entity is performing each action. Amended claim1 recites "at the registration authority, receiving a request from a principal to issue a certificate on behalf of that principal; and forwarding said request to a certification authority, wherein said request includes a first identifier that identifies the registration authority..."

In the de Silva patent the local server generates the request, as noted by the examiner, and corresponds to the recited registration authority. The examiner admits that the de Silva patent does not disclose that the certificate generated by the certificate authority includes any information identifying the local server (202). However, the examiner claims that the Hind patent discloses a certificate that contains a device identifier and that this device identifier is equivalent to the recited registration authority identifier.

In Hind, an administrative server makes the request to the certificate authority for the certificate and, thus, corresponds to a registration authority as recited in claim 1. Although the administrative server forwards an identifier along with the request, this identifier is for a mobile device that is associated with the administrative server. The

examiner claims that the mobile device is a requesting node. However, it is clear in hind that the administrative server drives the process, first, by requesting an identifier from the mobile device and then forwarding that identifier along with a request for a certificate to the certificate authority. See Hind, column 9, lines 16-43. Since the administrative server controls many mobile devices, the certificate that is generated does not tie the certificate to the administrative server. Therefore, if the administrative server becomes untrustworthy, the identifier in the certificate cannot be used to quickly revoke certificates requested by it. Consequently, the Hind arrangement cannot solve the problem to which the present invention is directed.

Rather than teaching or suggesting that de Silva's certificate include an identifier for the local server, the proposed combination would teach that the de Silva certificate should include an identifier for the client, since the client in de Silva most closely corresponds to the mobile device in Hind. Since neither de Silva nor Hind is directed to the problem solved by applicant's invention – identifying a node that makes a request for a certificate so that the certificate can be more easily revoked, the combination could not suggest substituting an identifier for the local server or the administrative server for the mobile device identifier actually disclosed in Hind.

The present claims particularly point out this difference. For example, claim 1 recites, in lines 7-12, "forwarding said request to a certification authority, wherein said request includes a first identifier that identifies the registration authority and at the certification authority ...generating a certificate that includes said first identifier." As discussed above, neither de Silva nor Hind discloses that the server which makes the certificate request to the certificate authority makes a certificate request which includes an identifier identifying the server. Nor can the combination of these references suggest this recited combination also as discussed above. Thus, claim 1 patentably distinguishes over the cited combination of references.

Claims 4, 5, 7, 9 and 11 are dependent, either directly or indirectly, on claim 1 and incorporate the limitations thereof. Claims 4, 5, 9 and 11 have been amended to conform them to changes made in amended claim 1. Therefore, they distinguish over the cited combination of references in the same manner as claim 1. In addition, these claims recite limitations not taught or suggested by the cited combination of references.

For example, claim 7 recites that the certificate includes a time stamp associated with the request. The examiner claims that a timestamp is inherent in de Silva because de Silva discloses checking the expiration date of a certificate and a timestamp is required for that purpose. Assuming that to be the case, any such timestamp would be associated with the certificate issuance date rather than with the request date. Nonetheless, the examiner claims that it would have been obvious to include a timestamp in the certificate that refers to the request. However, the examiner does not point to any reference that shows such a timestamp or suggests such a timestamp. If the examiner is relying on art known to her or to general knowledge in the art , she is respectfully requested to identify such art or the source of such general knowledge.

Claim 17 distinguishes over the cited combination in the same manner as claim 1. For example, claim 17 recites, in lines 6-10, "receiving a request from a registration authority to issue a certificate on behalf of a principal; and in response to receipt of said request, generating said certificate that includes at least a registration authority identifier associated with said registration authority." As discussed above, neither de Silva nor Hind discloses that a generated certificate include an identifier associated with a server that might correspond to the recited "registration authority", such as the de Silva local server or, possibly, the Hind administrative server. Nor can the combination of these references suggest this recited combination also as discussed above. Thus, claim 17 patentably distinguishes over the cited combination of references.

Claims 18 and 20 are dependent on claim 17 and incorporate the limitations thereof. Therefore, they distinguish over the cited combination of references in the same manner as claim 17. In addition, these claims recite limitations not taught or suggested by the cited combination of references. For example, claim 20 recites that the certificate includes a timestamp associated with the request in a manner similar to claim 7. Therefore, claim 20 distinguishes over the cited combination of references in the same manner as claim 7.

Claim 34 contains limitations that parallel those in claims 1 and 17 and distinguishes over the cited combination of references in the same manner as claims 1 and 17. Claims 36 and 37 are dependent on claim 34 and incorporate the limitations thereof. Therefore, they distinguish over the cited combination of references in the

same manner as claim 34. In addition, these claims recite limitations not taught or suggested by the cited combination of references. For example, claim 37 recites a means that provides an indication that a certificate is untrustworthy based on a comparison of a node identifier in the certificate with the node identifier of an untrustworthy node on a certificate revocation list. The examiner points to de Silva as disclosing revocation of certificates. However, de Silva does not disclose how the certificates are revoked as recited in claim 37. Consequently, de Silva does not disclose the limitations in claim 37 and claim 37 patentably distinguishes over de Silva and Hind.

Claims 2-3, 6, 10, 19 and 35 have been rejected under 35 U.S.C. §103(a) over de Silva in view of Hind and further in view of U.S. Patent No. 6,308,277 (Vaeth, previously cited.) Claims 2, 3, 6 and 10 are dependent on claim 1 and incorporate the limitations thereof. These claims distinguish over the combination of de Silva and Hind as discussed above. Adding Vaeth to the combination does not supply the limitations that are missing in the combination of de Silva and Hind. In particular, Vaeth discloses a certification system that includes a registration authority and a certificate authority. However, as discussed in the immediately preceding response, Vaeth does not disclose or suggest that the registration authority, which makes the certificate request to the certificate authority makes a certificate request which includes an identifier identifying the registration authority as recited in claim 1. Therefore, the certificate returned to by the certificate authority does not include this identifier also as recited in claim 1. Consequently, claims 2, 3, 6, and 10 distinguish over the cited combination in the same manner as claim 1. Claims 2, 3, 6 and 10 have been amended to conform them to the changes made in amended claim 1.

In the same manner, claim 19 is dependent on claim 17 and claim 35 is dependent on claim 34. As discussed above, claims 17 and 34 distinguish over the cited de Silva and Hind combination. Since adding the Vaeth reference to this latter combination does not change the combination such that it would render claims 17 or 34 obvious, claims 19 and 35 also distinguish over the cited combination.

Claims 28-33 have been rejected under 35 U.S.C. §103(a) over de Silva in view of Vaeth. Vaeth is discussed above. It does not disclose the registration identifier.

Claim 28, for example, recites "program code ... for generating by a certification authority a certificate ... includes ... a registration identifier associated with said registration authority." Thus, claim 28 patentably distinguishes over the cited combination of de Silva and Vaeth. Claim 29 depends on claim 28 and, therefore, incorporates the limitations of claim 28 and patentably distinguishes over the cited combination in the same manner as claim 28. Claim 30 contains limitations that parallel those in claim 28 and distinguishes in the same manner. Claims 31-33 depend on and incorporate the limitations of claim 30 and thus distinguish over the cited combination in the same manner as claim 30.

In light of the forgoing amendments and remarks, this application is now believed in condition for allowance and a notice of allowance is earnestly solicited. If the examiner has any further questions regarding this amendment, she is invited to call applicants' attorney at the number listed below. The examiner is hereby authorized to charge any fees or direct any payment under 37 C.F.R. §§1.17, 1.16 to Deposit Account number 02-3038.

Respectfully submitted

Paul E. Kudirka Date: 9/19/05

Paul E. Kudirka, Esq. Reg. No. 26,931
KUDIRKA & JOBSE, LLP
Customer Number 045774
Tel: (617) 367-4600 Fax: (617) 367-4656